MSNBC.com

Is your personal data next?

Rash of data heists points to fundamental ID theft problem

ANALYSIS
By Bob Sullivan
Technology correspondent
MSNBC
Updated: 10:39 a.m. ET April 28, 2005

Another day, another massive data leak. Another 100,000 or so Americans exposed to identity theft. And still, we don't seem ready to talk about the real problem: Consumers are being forced to live in the personal data flood plain, often against their will. And the river keeps rising.

What's more, however bad the news may sound now, the size of the problem has been generally underestimated . Companies have shown a tendency to lowball the size of the data theft flood in their initial disclosures. For example:

- On Feb. 14, ChoicePoint Inc. said its data theft involved 30,000 to 35,000 people, and only California residents were involved. Only later did the firm admit the crime involved about 150,000 people all around the country.
- On March 9, LexisNexis said information about 30,000 people had been stolen from its databases. The number was revised upward to 310,000 on April 12.
- DSW Shoe Warehouse told the world 100,000 credit card numbers were stolen in early March, only to reveal last week that the true size of the theft was more like 1.4 million.

The data loss flood isn't just a problem for corporate America, either. More than 100,000 people were exposed by data thefts at The University of California at Berkeley, and at Boston College. Other massive data thefts at Chico State in California, George Mason University, and the Las Vegas Department of Motor Vehicles each exposed tens of thousands of consumers. In Las Vegas, criminals actually drove a car through an external wall in the building to race inside and steal blank IDs and data.

The obvious question must be asked -- at some point, will everyone's identity be stolen?

That's not as far fetched as it sounds. The Federal Trade Commission estimates that 27 million Americans were victims of some kind of ID theft in the past five years. Other studies suggest 1 in 20 U.S. citizens had been hit by this kind of electronic fraud. Last year, an industry group suggested that about 100 million credit card numbers had been stolen in one way or another.

The numbers are staggering. Just adding up the news from 13 recent high-profile data theft incidents shows 5.2 million consumers were exposed to identity theft through data leaks. It's undeniable that high-tech financial firms are selling, sharing, and hemorrhaging personal data like a leaky dam. But yelling at the leaky dam won't do much good, and neither will spackling over the holes. A more fundamental change is needed.

The data is too valuable

Theft of personal data is prevalent for one simple reason: the data is incredibly valuable. It's time Congress and U.S. financial institutions take an honest look at why that is, an honest look at the only reason anyone wants to steal all that personal data in the first place: the free-flowing, overflowing issuance of instant credit.

Economic Affairs Committee Meeting
June 24, 2005

Today, consumers can walk into virtually any electronics store with an empty wallet and walk out with a $3,000 television set in a few moments. Often, all that's required is a Social Security number that happens to be attached to a decent credit rating. As long as these stolen nine digits are worth $3,000 or more, criminals will always find a way to take them.

Only meaningful reform of the way our nation distributes instant credit will change this equation. Hackers will always steal what's valuable; only by de-valuing personal information like Social Security numbers will the rash of high-tech data thefts stop.

The credit and retail industries fear any interruption in the free-flow of credit, saying it will cut down on consumer impulse buys. So we sacrifice the privacy of millions to protect the ability to spend much of our future earnings in an instant. It's time to openly debate the wisdom of that trade-off.

Beating up ChoicePoint doesn't solve the problem

Companies like ChoicePoint have taken a public beating in recent weeks, with government officials critical of the firm's data gathering and storage practices.

While it's clear ChoicePoint and the other companies involved in data leaks didn't do enough to secure the private information it stores, beating up these organizations will do little really to stop the problem of identity theft. Criminals will just find another source of the data. Congress will continue to hold hearings, and debate measures such as limitations on the sale of Social Security numbers. That's a step worth exploring, but it will only stop legal sale of SSNs. Illegal data sales, and thefts, will continue unabated -- as long as the data remains so valuable.

While federal legislators have yet to take on easy access to instant credit, many state legislators are doing just that. About 20 states are considering laws that would allow consumers to lock down their credit reports, preventing anyone from obtaining instant credit by using their personal information. It's called a security freeze.

Such laws would not prevent data theft; but they would make stolen data much less valuable to the thieves. For those who have already been victims of identity theft, placing a security freeze on credit files offers an instant source of comfort. Those at high risk for ID theft, such as those going through divorce or those facing domestic violence, may also find the measure comforting.

One might think a law that require people to stop and think for a moment before making a big purchase like a house, car, or plasma TV could find supporters among retailers and creditors concerned about deadbeats. After all, the industry spent years begging Congress to pass a law that would make it harder for consumers to declare personal bankruptcy. Because a security freeze must be "thawed" ahead of any credit purchase, it would require consumers to think ahead more, and could promote better financial planning.

Instead, lobbying efforts by the credit and retail industries have helped kill freeze bills in four states.

But credit freezes are taking hold in other places. All Californians and Texas residents who have been victims of identity theft already have the right to a security freeze. Louisiana and Vermont residents will be able to implement freezes once those states' laws take effect on July 1. And Washington state legislators passed their version of the law last week. Legislation in about 15 other states is still being considered.

The credit industry is correct that many consumers may choose not to take the extreme step of a credit file lock. In California, only 4,000 people have filed for freezes so far, though many consumer advocates say that's because most consumers don't know they have the option.

But even if the choice is deliberate, giving consumers that choice is critical. Many consumers choose today to not lock their car doors. But the auto industry has repeatedly responded to the problem of auto theft, adding electronic devices, car stereo face plates, and electronic ignition keys. There are a host of things consumers can do to decrease the odds that their car will be stolen. Not so with their identity.

Consumers needs a choice

America's credit industry must offer consumers similar choices. Today, there is nothing a consumer can do to prevent an episode of identity theft. Personal data lands on the computers of firms such as ChoicePoint without the consent of the consumer. It may then be stolen without their knowledge. The best a consumer can do is find out after an identity theft is already under way.

If the last six weeks' worth of database heists have attracted any meaningful attention to the problem, federal legislators and financial institutions must recognize that the dam of personal information is broken. It's a question not of if, but when, their personal information will flow over the banks during the next data leak.

Given that reality, people need a tool that them to lock the doors on their digital lives. Consumers deserve the option to move their personal information out of the identity theft flood plain, up to high ground.

Bob Sullivan is author of Your Evil Twin: Behind the Identity Theft Epidemic

© 2005 MSNBC Interactive

© 2005 MSNBC.com

URL: http://www.msnbc.msn.com/id/7358558/